Security challenges in Industrial Internet Of Things

Luca Hohmann

16.04.2022

1 Introduction

Today's information systems contain many different security and privacy related technologies and techniques in order to facilitate for the ever looming threat of malicious attackers. Especially through attacks on big corporations and institutions within recent history (Hardcastle 2021), information security and information privacy have gained the attention these fields have been lacking in the past years. While the traditional field of information security is now picking up tracking, a different field of cyber security is emerging in front of the world. The decentralized, Industrial Internet Of Things (IIOT) is gaining foothold in businesses and manufacturers around the globe. Because the IIOT consists of thousands, to hundred of thousands of devices per business, a completely new approach to security must be provided in order to deal with the given requirements and constraints of the newly developing technology. While this IIOT can increase the potential and productivity of many businesses, it may also cause catastrophic failures for others if not executed and secured properly. Therefore this survey focuses on security of the IIOT and in more detail about potential attestation methods for IIOT devices being deployed in the future.

In the following section, the IIOT is described in the necessary details to then understand general information security concerns and problems for the domain according to other literature. Afterwards a more detailed problem statements and solutions for the attestation technology for IIOT networks are synthesized from existing literature about the topic and related areas. Lastly a conclusion describes the key takeaways and developments for the future to monitor more closely.

2 Industrial Internet and security

2.1 Industrial Internet

The industrial internet is a technology trend, which until now has just started gaining traction. It is party of the Industry 4.0 and will increase productivity, performance and profits by magnitudes larger than other recent innovations. It is built upon three key components: Intelligent machines, advanced data analytics and people on site and remotely who interact with these former two

components (Evans and Annunziata 2012). Businesses around the world, especially manufacturers, want to use digitalization through high number deployment sensors, smart devices and microprocessors in the IIOT. In order to use the maximum potential of data generation by monitoring, and the following potential of big data analysis in order to gain insights into their business processes, the amount of devices deployed and communicating with each other must be widespread across the business facilities. This allows processes to be further improved through digital and human cooperation and drive businesses to new fields of expertise and improving their performance in their current respective area of business. Especially in the area of product customization through software, every business can accustom many more customers and tailor products to every single buyer's needs. This allows customers to gain maximum profit and effectiveness out of products they buy, as the digital aspects of these smart devices can and will continue to develop for the whole life time of the product (Porter and Heppelmann 2015). These trends power the Industry 4.0 and lie the foundation of the Industrial Internet.

2.2 General Security Challenges in IIOT

The IIOT is a network of devices which expands beyond the size of any current day corporate networks. It not only consists of classic information systems like user workstations, internal and external service providing server, but also of many heterogeneous internet of things (IoT) devices. These IoT devices, not consisting of traditional consumer product IoTs, but industrial IoT products, can span a wide range of hardware platforms, software stacks, behaviours, resources and possibilities. These devices place physical restrictions and requirements onto any potential solution for securing them, digitally as well as physically and their respective communication with other devices within the network. In addition to single device restrictions, the amount of devices placed in facilities can potentially reach thousands of devices for major production plants with over 100 billion devices for all businesses globally in 2016 (PWC 2016).

In order to later understand the attempt to attest devices in these hyper complex mesh networks, first some basic security concepts and problems for the IIOT are explained in more detail.

2.2.1 Cryptography in the IIOT

One of the fundamentals of security is the cryptography. It allows humans and machines to provide confidentiality for data, so preventing 3rd parties from accessing data, and at the same time can be used to authenticate parties to each other through signature schemes. In the IIOT the full palette of cryptography must be used in order to provide confidentiality, integrity and available, as well as additional security and privacy requirements. However cryptography nowadays works by using key material of different lengths, depending on the scheme, in order to perform operation on data. These operations take time, are expensive in terms of memory usage and power consumption (Zhou et al. 2018). However IIOT devices, which are deployed outside of the internal IT network usually consist of microcontroller based systems, with no access to power

sources, major computational resources or hardware accelerators. Therefore the devices can only perform these expensive cryptography algorithms in a slow matter in order to communicate, authenticate and proof correctness with other devices (Sadeghi, Wachsmann, and Waidner 2015) (Zhou et al. 2018). This becomes a problem for these devices as their original purpose is to provide real time data to other devices within the network. These amounts of data are used for data analysis, communication between different sensors and automated decision making by machines. If the data cannot arrive in real time or in a safe manner, potential risks involve stalling of production, safety and security risks for machines and humans as well as theft of valuable, private data (Serror et al. 2021).

Therefore a subfield of cryptography is developing, where hyper-efficient yet secure encryption schemes are researched and developed in order to replace the otherwise state of the art cryptography schemes, currently too slow for the IIOT requirements. Many different approaches can be taken, from trying to improve current methods with better underlying mathematical procedures (Bernstein et al. 2012) to precomputing parts of the encryption due to communication patterns of devices with others (Hiller et al. 2018) or building completely new cryptographic algorithms (Jérémy et al. 2016). While none of the approaches alone will fully solve all issues, a combination of many different ones could proof to be an efficient, yet secure solution. However these must then be standardized and adopted in a way that heterogeneous networks can use the same cryptographic primitives and techniques in order to allow a unified and more manageable and scalable network.

2.2.2 Securing devices in a mesh network

Any IIOT network of the future must be easily scalable and be able to be secured against physical attacks. Physical attacks can occur in two different ways. Either the malicious actor gets hold of a legitimate device within the network and is able to attack it through various methods, or the attacker can add a malicious device to the existing network. These two types of attacks rely on the physical security of the deployed devices and the network and wireless communication these devices employ in the network.

In order to protect devices against the first type of attacks, where a malicious actor gets hold of a legitimate device and tries to tamper with it or receive secret data from it via reverse engineering, a multitude of security mechanisms can be deployed. An uprising technology is secure computing, which in desktop and server level processing units consist of Intel SGX (Intel n.d.) and ARM TrustZone (ARM n.d.). These secure computing areas protect computations against reverse engineering through cryptography schemes and make it very difficult to tamper with data and code inside of it due to high confidentiality and integrity guarantees. However these technologies require a lot of resources, including extra hardware, more power supply and computation time (Sadeghi, Wachsmann, and Waidner 2015). Therefore they are not easily applicable to IIOT devices, as their resources are limited and their main goal is to provide real time data processing. Instead of providing security guarantees to all application which use these trusted execution environments, different more goal oriented execu-

tion environments have been developed. As adeghi, Wachsmann, and Waidner (2015) have described in their survey, these other execution environments, such as SMART (Eldefrawy et al. 2012) or TrustLite (Koeberl et al. 2014) can all provide certain guarantees to applications. However all of them come with limitations, making the decision process a lot harder for the companies developing the IIOT devices.

Additionally a lot of different manufacturers might use all kinds of execution environments, so compatibility between devices and their security guarantees cannot be universally described. Therefore a small, common set of trusted environments should be used as standards in order to allow companies to focus on very few of these technologies instead of trying to work with potentially dozens of different security parameters in their anyway highly heterogeneous network.

Not only can attackers try to attack existing devices, but due to the constantly expanding number of devices in a potential factory of the IIOT, the attacker can also attempt to add their own, malicious device to the network. This kind of attack becomes more and more prevalent with the usage of Bluetooth technology. The problem with this technology is the addition of new devices, which can be reasonably secure if they are manually verified during the pairing process, but cannot be considered secure if an interfaceless device is added via pairing. The problem with machine pairing in bluetooth is that devices do not need a human verification of exchanged codes and therefore any device can join the network. At the same time, these IIOT devices should not employ human interfaces in order to save resources for a longer product lifetime and faster computation and data transferring. However this allows attacker to infiltrate the network with malicious devices if no other protection mechanisms are employed. One highly interesting approach has been designed by Miettinen et al. (2014), where devices use common sensors to identify whether a newly added device is within the same area and therefore a trusted device (see Figure 1). Instead of immediately trusting the newly device after one checkup, a continuous protocol has been adopted, which over time adds more trust to the new device. This makes it harder for attackers to generate the required data with an algorithm. The data that these devices can use to identify their area can depend on many different sensors. Audio based sensors can be used to listen for similar sound signals. Temperature and humidity sensors are available to check for the room temperature and humidity. Lighting sensors can be used to identify the amount of incoming light in the area and many more. The data from these sensors are then exchanges through the protocol and in form of challenge and response required from the newly added device. Only if the provided data lies within a reasonable range of error. This approach allows it to add new devices to the network in a more secure way than simply connecting it via a wireless technology without any security guarantees.

While Miettinen et al. (2014)'s approach is a great improvement over current standards for interfaceless device installation, the security is solely based on the assumption that the area is restricted and cannot be accessed by malicious actors. However internal actors, with access to the area might be able to install a maliciously tampered device in the company facility without someone noticing

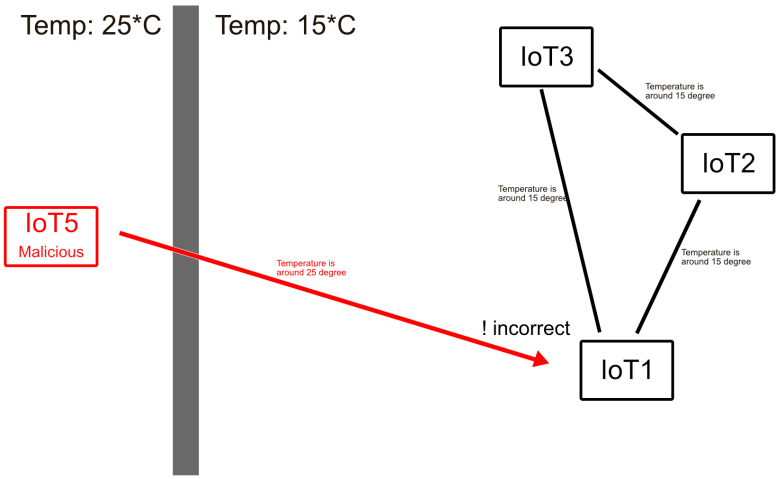

Figure 1: Attempt of malicious IoT device to join the network with incorrectly measured temperature

it before it is too late. Therefore companies should not only rely on this system, but use it in combination with potential other solutions and monitoring systems in order to check how many devices are actually installed and how many there should be.

3 IIOT Integrity: Attestation

While the above security concerns are major parts of the security architecture of IIOT networks, one area that has not yet seen as much research in the security area is the integrity protection of IIOT devices. Integrity protection refers to mechanism providing reliable information about a system to identify whether it has been tampered with. This area of security is usually resolved via checksum calculations and attestation of properties. The former method is often used when software is installed and the user wants to verify whether the file has been modified during the download from the web. So the software provider also offers a calculated checksum, a hash function result, and then required the user to calculate the hash function for the program himself in order to verify that both results are the same and the file has not been modified.

This static approach for files and data can be taken into dynamic execution of software and hardware properties. The so called attestation of properties of software and hardware is done by a third party, either remotely or directly on system in order to check whether the current state of the machine matches an expected, precomputed state by the so called verifier. This system is called attestation and is likely to play a big rule in IIOT deployment. Due to the high number of devices deployed and the various locations these can be deployed at, it is highly suggested that devices are also integrity protected on their hardware as well as software level. If any malicious actor then tries to tamper with the

device, the attestation system is able to detect these integrity violations and stop any execution before malicious activity can create damage in the device or network. This also adds inherent security to the device, even if it is in a non secure location (see 2.2.2). For attestation to work, the previous security problems have to be resolved for IIOT devices, as otherwise no guarantees about devices can be made. For example a maliciously added more powerful devices, which has not been detected yet, can verify that it runs some reverse engineered sensoring code correctly, while at the same time sending out malicious network packages to attack the whole network. Therefore the base layers of security and management of the network have to be set in order to be able to apply attestation in a useful manner. While in day to day computing systems these attestations are already available via secure hardware such as Trusted Platform Module (Microsoft 2022), this kind of technology is not available for IIOT devices with the limited resources and computational power. Additionally software based attestation is possible, however it is questionable whether this kind of attestation holds much value, due to the fact that code can be changed by an attacker when it is not used with a secure computation environment like Arm TrustZone, Intel SGX, SMART or TrustLite. However due to the major resource constraints, most of the IIOT attestation based researched methods still rely on some kind of software based attestation with some involvement of hardware features. While for IoT systems different kinds of remote attestation techniques have been researched and implemented in recent years (Tan, Tsudik, and Jha 2017) (Conti, Dushku, and Mancini 2019) (Moreau, Conchon, and Sauveron 2021), they either relate to more powerful IoT devices or try to shift attestation from the less powerful devices to the more powerful devices. However due to the sheer amount of heterogeneous devices and their requirement of providing real time data output and at the same time, without creating major delays in data flow, proving their integrity, these methods are not easily applicable.

One area that has gained lots of attention in recent years is swarm based attestation inside of IIOT networks. The idea of the swarm based attestation is built upon the mesh network topology many IIOT networks are likely to employ. So instead of verifying every node, a verifier checks a subset of nodes randomly for different aspects, such as checksums data flow between nodes and their current executions. Additionally distributed attestation from one node to another is possible with schemes such as ESDRA (Kuang et al. 2019). The possible advantage of these distributed and swarm based attestation methods is a quite high security level, despite using mainly software based attestation methods, by always randomizing the set of nodes to be attested at any given time. This allows devices to spend more computational power on the actual task they have to perform, instead of constantly verifying themselves against the verifier. The main reason such a swarm based attestation is possible is the homogeneity of the datastream that is expected to arrive at the central data collector. Because the machines that are monitored should run in normal operations mode within a certain range of measurable values. If the data provided by the IIOT devices changes massively, it could be indicated that either the device that is monitored through the sensor has a fault or something is wrong with the IIOT device. So once this occurs, the verifier could then specifically target this IIOT device to make an on demand attestation for the device to rule out any manipulation

attempts by attackers.

While swarm attestation seems like a good compromise between security and practicability, the attestation area is yet to be more researched and developed. Especially the only partially hardware based integrity protections are yet to be improved with the previously mentioned hybrid secure execution environments like TrustLite and SMART and potentially newly upcoming developments from the hardware manufacturers. Additionally new attestation methods, which can also just guarantee the correct execution of algorithms, while being done on a otherwise not securely guaranteed device are currently researched via stack based execution verification. This topic is especially interesting as it will cover the master thesis of myself in the upcoming autumn and winter. Using such verification methods could additionally prove very useful for IIOT devices, as then hardware based integrity protections can be leverages at the level they currently are, but do not require any major upgrades, as the algorithm itself is then protected via attestation.

4 Conclusion

The security research for IIOT devices is gaining more and more traction as researchers and companies realize that they need to set the fundamental security practices early on before too many unsecure devices and networks are built. Otherwise it will be too late again to create proper it-security and firefighting against vulnerabilities and hacks in facilities around the world is going to occur at unprecedented frequencies. Therefore all areas of security for small, resource restrained devices should be researched, adopted and implemented as soon as possible with as much standardization as possible. In the survey above several security techniques have been shown and discussed and many more are available. In the future IIOT device might be properly secured for a safe and secure industrial internet.

References

ARM (n.d.). *ARM TrustZone*. URL: `https://www.arm.com/technologies/trustzone-for-cortex-a`.

Bernstein, Daniel J et al. (2012). "High-speed high-security signatures". In: *Journal of cryptographic engineering* 2.2, pp. 77–89.

Conti, Mauro, Edlira Dushku, and Luigi V. Mancini (2019). "RADIS: Remote Attestation of Distributed IoT Services". In: *2019 Sixth International Conference on Software Defined Systems (SDS)*, pp. 25–32. DOI: `10.1109/SDS.2019.8768670`.

Eldefrawy, Karim et al. (2012). "SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust." In: *Ndss*. Vol. 12, pp. 1–15.

Evans, Peter C and Marco Annunziata (2012). "Industrial Internet: Pushing the Boundaries of Minds and Machines". In: *General Electric* June, p. 37.

Hardcastle, Jessica Lyons (2021). "Worst Cyberattacks of 2021 (So Far)". In: *sdx central*. URL: `https://www.sdxcentral.com/articles/news/worst-cyberattacks-of-2021-so-far/2021/12/`.

Hiller, Jens et al. (2018). "Secure low latency communication for constrained industrial IoT scenarios". In: *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*. IEEE, pp. 614–622.

Intel (n.d.). *Intel SGX*. URL: https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html.

Jérémy, Jean et al. (2016). "Deoxys v1.41". URL: https://competitions.cr.yp.to/round3/deoxysv141.pdf.

Koeberl, Patrick et al. (2014). "TrustLite: A security architecture for tiny embedded devices". In: *Proceedings of the Ninth European Conference on Computer Systems*, pp. 1–14.

Kuang, Boyu et al. (2019). "ESDRA: An Efficient and Secure Distributed Remote Attestation Scheme for IoT Swarms". In: *IEEE Internet of Things Journal* 6.5, pp. 8372–8383. DOI: 10.1109/JIOT.2019.2917223.

Microsoft (2022). *Trusted Platform Module Technology Overview*. URL: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview.

Moreau, L., E. Conchon, and D. Sauveron (2021). "CRAFT: A Continuous Remote Attestation Framework for IoT". In: *IEEE Access* 9, pp. 46430–46447. DOI: 10.1109/ACCESS.2021.3067697.

Porter, Michael E and James E Heppelmann (2015). "How smart, connected products are transforming companies". In: *Harvard business review* 93.10, pp. 96–114.

PWC (2016). *The Industrial Internet of Things*. Tech. rep. URL: https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf.

Sadeghi, Ahmad-Reza, Christian Wachsmann, and Michael Waidner (2015). "Security and privacy challenges in industrial Internet of Things". In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6. DOI: 10.1145/2744769.2747942..

Serror, Martin et al. (2021). "Challenges and Opportunities in Securing the Industrial Internet of Things". In: *IEEE Transactions on Industrial Informatics* 17.5, pp. 2985–2996. DOI: 10.1109/TII.2020.3023507.

Tan, Hailun, Gene Tsudik, and Sanjay Jha (2017). "MTRA: Multiple-tier remote attestation in IoT networks". In: *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9. DOI: 10.1109/CNS.2017.8228638.

Zhou, Lu et al. (2018). "Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints". In: *IEEE Signal Processing Magazine* 35.5, pp. 76–87. DOI: 10.1109/MSP.2018.2846297.